David Morfe

Professor Qiu

CS351 - Intro. to Cybersecurity

17 November 2020

**Project Milstone November 17th**

My project's back end is written in Python's Flask framework and front end written in JavaScript, HTML & CSS. So far I have already created my databases and organized the source code files I'll be developing. This end to end secure messaging system will be a web app with the back end server handling all the client interactions and message communication.

The first module, the user resgitration and authentication compenent, will composed on an index page. With a generic username password login form, registration button and possibly a forgot password button. Users will login with their credentials they registered with and the data will be sent as a post request to the back end server. Password will be hashed and stored that way in the database with salt.

The second module, server authentication and user account managment incorporate three different databases. Users, Friends, Channels. Users will have basic user information and email for verifying the user is who they are their identity using 2 factor verification. To be sure users are talking to the right server each client will be put in a session once logged in.

The third module, for secure user communication will be handled with sessions and the Friends and Channels database. The Friends database shall keep track of the friends each user can comminicate. Once a chat is initiated, the chat channel's randomized ID will be stored in each client's session to be sure only the clients on both ends can use said channel. The Channels database will keep track of all the channels, the users that can access them and the chat log itself. I also plan on implementing public key authentication. generating public keys and private key pairs than can only be decrypted by server side.